COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

May 9, 2013

TO: Marvin J. Southard, D.S.W., Director
Department of Mental Health

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT COMPLIANCE REVIEW – COMPTON FAMILY MENTAL HEALTH CENTER**

We have completed a Health Insurance Portability and Accountability Act (HIPAA) compliance review of the Department of Mental Health (DMH) Compton Family Mental Health Center (CFMHC), a HIPAA covered facility. Our review was prompted by prior findings of non-compliance during an unannounced site visit to CFMHC. This report details our findings and recommendations for corrective action.

Background

On November 15, 2012, we conducted an unannounced visit to CFMHC as our efforts to ensure that the County's HIPAA covered programs and clinics are posting their Notice of Privacy Practices (NPP) in prominent patient locations, as required. We noted that CFMHC did not post the NPP as required. In addition, the facility manager did not know what a NPP was, or where hard copies of the NPP were located, indicating a lack of management knowledge and accountability for core HIPAA requirements. These findings prompted a full HIPAA compliance review of CFMHC.

Our review evaluated CFMHC's compliance with the HIPAA Privacy Rule and DMH's HIPAA policies and procedures. We also used the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Act Audit Tool* in evaluating the facility's compliance. DMH management is responsible for establishing and maintaining internal compliance with the HIPAA regulations, and has oversight of their HIPAA compliance throughout DMH facilities. We considered DMH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could have a direct and material effect on CFMHC.

Summary of Findings and Recommendations

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity, such as the County, with direct treatment relationships with patients to give the NPP to every patient no later than the date of first service delivery, and to make a good faith effort to obtain the patient's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where health care is provided directly to patients, the provider must also post the notice in a clear and prominent location where patients are likely to see it, as well as make the notice available to those who ask for a copy.

Our follow-up review from the November 15, 2012 unannounced visit found that the facility posted the NPP in the patient waiting area where patients and visitors are likely to see it. CFMHC management affirmed that all patients are provided with the NPP on their first service delivery date. We reviewed five randomly selected patient charts, and noted they all included the acknowledgement.

While CFMHC was not in compliance with the NPP standards at the time of our unannounced site visit in November 2012, the facility addressed the deficiencies in this area and was fully compliant at the time of this review.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of protected health information (PHI). A covered entity must reasonably safeguard PHI and electronic PHI, and make reasonable efforts to prevent any intentional or unintentional use or disclosure that violates the Privacy Rule.

We reviewed DMH's Policy Number 500.21, *Safeguards for Protected Health Information*, which establishes administrative, physical, and technical safeguards to protect the confidentiality of PHI. We also reviewed DMH's Policy Number 302.14, *Networked Information Systems Usage*, which governs the use of DMH information technology resources and communicates to DMH workforce members their responsibility for acceptable use of DMH information technology resources.

CFMHC management reported that their computers are protected by endpoint protection software, which blocks downloading of PHI to a portable storage device. In addition, CFMHC computers are configured to prevent workforce members from saving PHI onto their hard drives.

During our review, we noted that computer monitors of front office staff are in plain view of visitors and/or patients, which could result in the inadvertent disclosure of PHI. We

also noted that medical records are stored in the basement of the building, and that access is appropriately restricted to authorized CFMHC staff.

CFMHC management reported that the facility uses Accutrac to track the flow of medical charts, but that the software is disabled due to computer upgrades. Consequently, charts are currently being tracked manually by the custodian of records. To ensure that all files are accounted for, the custodian of records will search for charts that are not returned by the end of the business day.

Because front office staff computer monitors are visible to visitors and patients, which could compromise PHI, CFMHC is in partial compliance with the Physical Safeguards standards. To the extent that we were able to review CFMHC's administrative and technical controls over PHI, the facility appears to be in compliance.

Recommendation

1. **CFMHC management install privacy screens on monitors that are in plain view of patients and/or visitors, or implement alternate safeguards, to prevent inadvertent disclosure of PHI.**

Training

The CFMHC, as a covered facility, must train its entire workforce on policies and procedures related to PHI that are required by the HIPAA Privacy and Security Rules, and to the extent necessary and appropriate for the members of its workforce to carry out their functions. Members of the workforce include employees, volunteers, and trainees.

The DMH Human Resources Division is responsible for ensuring its workforce members receive general HIPAA compliance training, and the Department's HIPAA policies and procedures via the Learning Net. CFMHC management is responsible for providing additional role-based training for their workforce members.

Our review of CFMHC HIPAA training records noted that CFMHC is not in compliance with the training standards. Six (13%) of 46 workforce members have not met the training requirement. Four of the six workforce members who have not met the training requirement are on long-term leave.

Recommendation

2. **CFMHC management must implement a corrective action plan to ensure that all workforce members meet the training requirement.**

Complaint Process

A covered entity must provide a process for patients to make complaints concerning the covered entity's policies and procedures. A covered entity must document all complaints received and their disposition, if any.

CFMHC management informed us that they currently follow DMH Policy Number 500.11, *HIPAA Privacy Complaints*, in handling patient complaints. Patients are directed to contact the Program Head or the Patients' Rights Office to file a complaint.

The CFMHC complaint process complies with HIPAA standards. We observed that the Program Head's name and contact information are posted on the registration window in the patient waiting area, to allow patients to voice their concerns regarding treatment or privacy issues. In addition, DMH's NPP, posted at the patient waiting area, informs patients that they may file a complaint with the U.S. Department of Health and Human Services (HHS), the County's Chief HIPAA Privacy Officer, or DMH's Patients' Rights Office. HIPAA complaint forms were available in the brochure racks at the patient waiting area.

Refraining from Intimidating or Retaliatory Acts

It appears that CFMHC is in compliance with the non-retaliation standards. Our discussions with CFMHC management confirmed they are aware of and understanding the importance of complying with DMH's Policy Number 500.18, *Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA.* Further, they understand that the Office for Civil Rights (OCR) will investigate any complaint against a covered entity that asserts retaliatory actions. No complaints related to retaliatory or intimidating acts were filed with the County's Chief HIPAA Privacy Officer by CFMHC patients in the past year.

Uses and Disclosures Requiring an Authorization

Guidance from the OCR states that an authorization is a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

CFMHC management indicated that workforce members have a general understanding of DMH's Policy Number 500.1, *Use and Disclosure of Protected Health Information Requiring Authorization*, and are following the policy. The purpose of our review was to

ensure that CFMHC is able to refer to its Department's policy regarding uses and disclosures of PHI.

The Department's revised *Authorization for Request or Use/Disclosure of Protected Health Information (PHI) form* was reviewed as part of this review and it meets the HIPAA requirements. It appears that CFMHC is in compliance with the Uses and Disclosures Requiring Authorization standards.

Accounting for Disclosures of Protected Health Information

A patient has a right to receive an accounting of PHI disclosures made by a covered entity, and covered entities must account for certain non-routine disclosures of PHI. The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, up to six years after the disclosure. The types of disclosures that are not required to be reported are disclosures: (1) to the patient, (2) for treatment, (3) payment and health care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures log must be maintained in each patient's medical chart.

CFMHC management reported that workforce members follow DMH's Policy Number 500.06, *Accounting of Disclosures of Protected Health Information,* account for all disclosures of PHI, including those with authorizations, and maintain logs in the certain patients' medical charts.

Our review of two patient accounting tracking sheets, provided by the facility, noted that the documentation meets the HIPAA requirements. It appears that CFMHC is in compliance with the Accounting for Disclosures of PHI standards.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Privacy Rule requires covered entities to make reasonable efforts to limit use, disclosure of, and any requests for PHI to the minimum necessary to accomplish the intended purpose for disclosure. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is reasonably necessary for a particular purpose.

Discussions with CFMHC management indicate that workforce members are aware of the minimum necessary standards. It appears that CFMHC is in compliance with the minimum necessary standards.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers, health plans, and other entities covered by the HIPAA to notify patients when their health information is breached. These "breach notification" regulations implement provisions of the HITECH Act, passed as part of the American Recovery and Reinvestment Act of 2009. The regulations, developed by HHS, require health care providers and other HIPAA covered entities to promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

CFMHC management informed us that they trained workforce members on their Departmental Policy Number 500.28, *Responding to Breach of Protected Health Information*, which provides clear guidelines and procedures to workforce members in the event a breach or suspected breach of PHI is discovered. We reviewed the policy and established that it provides proper guidance to workforce members. In addition, no breaches were reported from CFMHC to the County's Chief HIPAA Privacy Officer or OCR. It appears that CFMHC is in compliance with the HITECH Act Breach Notification standards.

Conclusion

Overall, our review indicates that CFMHC management is complying with HIPAA and HITECH Act requirements to protect patient confidentiality and safeguard PHI. DMH should take immediate action to address the deficiencies noted in this review, and report any corrective action taken or pending to the HIPAA Compliance Office within 90 days from the receipt of this memorandum.

We thank DMH's Audit and Compliance Division and CFMHC managers and staff for their cooperation and assistance during this review.

Please call Linda McBride at (213) 974-2166 or Julia Chen at (213) 974-8315 if you have any questions.

WLW:RGC:GZ:LTM:JC

c: William T Fujioka, Chief Executive Officer
John F. Krattli, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
Judith L. Weigand, Compliance Officer, Department of Mental Health
Veronica Jones, Privacy Officer, Department of Mental Health
Audit Committee
Health Deputies